REMARKS

Claims 1-24 were presented and examined. Claims 29-35 were previously withdrawn and claims 25-28 were previously cancelled. In response to the Final Office Action, no claims are amended, no claims are cancelled, and no claims are added. The Applicants respectfully request reconsideration in view of the following remarks.

I. Claims Rejected Under 35 U.S.C. § 103

Claims 1 and 14 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Roh and Kim, *"Security Model and Authentication Protocol in EPON-based Optical Access Network,"* ("Roh") in view of Examiner's Official Notice, and further in view of Atkins, et al. *"PGP Message Exchange Formats"* ("Atkins"). Claims 2-13 and 15-24 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Roh in view of Atkins in further view of "Cryptography and Network Security," by W. Stallings, 2nd Edition, 1999 ("Stallings").

To determine obviousness of a claim: (1) factual findings must be made under the factors set forth in Graham v. John Deere Co., 383 U.S. 1, 148 USPQ 459 (1966); and (2) the analysis supporting the rejection under 35 U.S.C. § 103 should be made explicit and there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. See MPEP §§ 2141(II), 2141(III), and 2142; KSR International Co. v. Teleflex Inc., 82 USPQ2d 1385, 1396. "If the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification." *In re* Gordon, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984).

In regard to claim 1, this claim recites "an optical line terminal for sending a discovery gate message to discover an optical network unit for data transmission, the discovery gate message including a public key of the optical line terminal" (emphasis added). The Examiner acknowledges that Roh does not disclose including a public key in the discovery message. See Final Office Action, Page 4. Instead, the Examiner takes Official Notice that "inclusion of an extra field in a message to include additional information was well-known in the art at the time of invention." *Id.* However, the Applicants submit that the modification of Roh based on the Examiner's assertion under his Official Notice, is improper.

Roh states "[i]n our protocol, the usage of the standard EPON MAC message containing ID and time-stamp fields *eliminates requiring the design of additional fields* or messages for the security mechanism in EPON" (emphasis added). Roh, § 4.2. The Examiner argues that a person of ordinary skill in the art would know that the standard EPON MAC message can be modified to include additional fields. However, modifying the traditional EPON MAC message to include an additional field for the public key would render Roh "unsatisfactory for its intended purpose," because the purpose of Roh was to develop a security structure which does not modify the standard EPON MAC message. See Roh, § 4.2. As stated above, "If the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification." *In re* Gordon, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984).

The Examiner further argues that a person of ordinary skill in the art would know that the standard EPON MAC message can be modified to include additional fields based on the teachings of U.S. Patent Application No. 2003/0147534 by Ablay *et al.* (hereinafter "Ablay"), U.S. Patent No. 6,105,012 issued to Chang (hereinafter "Chang") and U.S. Patent Application No. 2004/0255037 by Corvari *et al.* (hereinafter "Corvari"). These references disclose passing a public key in a data network. See Ablay, Paragraph [0040], Chang, Fig. 7 and Corvari, Paragraph [0042]. However, none of these cited references disclose modifying a standardized protocol to include a non-standard data component. Instead, these references disclose using proprietary message protocols to transfer public keys. Thus, the legal conclusion of obviousness lacks a rational underpinning as the argument presented by the Examiner is contradictory to the disclosure of the prior art.

In contrast, the key management device recited in claim 1 provides a more efficient security infrastructure by reducing the amount of messages required to initiate communications between a devices on an EPON while abiding by the constraints of the EPON MAC message protocol. Namely, in claim 1 a separate message is not required to transmit the public key of an optical line terminal during standardized EPON MAC communications.

Thus, for the reasons provided above, the Examiner's Official Notice was improper even in view of Ablay, Chang, and Corvari. Consequently, Roh fails to teach or suggest the cited elements of claim 1. Further, Atkins fails to cure the deficiencies of Roh. Therefore, claim 1 is not obvious in view of the combination of the prior art.

Further, claim 1 recites a procedure for providing a security service which is performed *during the authentication procedure*. Particularly, the public key is provided using the broadcast frame or the broadcast multicasting method.

Roh discloses a procedure of Key Distribution and Encryption which is performed during the final stage of ONU authentication (i.e. after the transmission of the registration message). That is, Roh is related to a procedure for providing a security service which is performed *after* the ONU authentication procedure. Further, the Examiner has not cited and the Applicants have been unable to locate any sections of Atkins which cure the deficiencies of Roh. By failing to disclose this element of claim 1, the combination of Roh and Atkins fails to disclose each element of claim 1.

Additionally, the public key of Roh is provided using a unicast frame rather than the registration message. Therefore, the registered ONU cannot determine whether the public key will be provided or not. Thus, when the public key is provided too late or not provided at all, the ONU cannot determine whether encryption of the REGISTER_ACK message and provision of a session key are necessary.

In comparison, claim 1 recites a procedure for providing a security service which is performed during the authentication procedure. As described above, Roh fails to disclose this element. Further, the Examiner has not cited and the Applicants have been unable to locate any sections of Atkins which cure the deficiencies of Roh. By failing to disclose this element of claim 1, the combination of Roh and Atkins fails to disclose each element of claim 1.

Moreover, Roh encrypts the whole Ethernet frame including Preamble (for providing LLID), when the Ethernet frame is transmitted after finishing the distribution of the public key and session key, because Roh processes the encryption procedure in a lower level of the MAC layer (i.e. Reconciliation Sublayer). However, the device of claim 1 encrypts only a part of the Ethernet frame. Specifically, the MAC address is not encrypted, because the device of claim 1 processes the encryption procedure in the MAC layer. Further, the Examiner has not cited and the Applicants have been unable to locate any sections of Atkins which cure the deficiencies of Roh. By failing to disclose this element of claim 1, the combination of Roh and Atkins fails to disclose each element of claim 1.

Lastly, in the protocol recited in claim 1, usage of the standard EPON MAC message containing ID and time-stamp fields eliminates the need for the design of additional fields or

messages to provide a security mechanism in an EPON. However, Roh requires the use of an additional field (i.e. the REGISTER_ACK message) for providing the session key. See RohRoh, § 4.2, page 402. Therefore the purpose of Roh, to develop a security structure which does not modify the standard EPON MAC message, is contradictory and cannot be used to meet the limitations of claim 1.

For at least the reasons provided above, the combination of Roh and Atkins fails to teach or suggest each element of claim 1. Accordingly, the Applicants respectfully request reconsideration and withdrawal of the rejection of this claim.

In regard to claim 14, this claim includes analogous limitations to those recited in claim 1. For at least the reasons described above, the combination of Roh and Atkins fails to disclose each element of amended claim 14. Therefore, claim 14 is not obvious in view of the combination of the prior art. Accordingly, the Applicants respectfully request reconsideration and withdrawal of the rejection of this claim.

Claims 2-13 and 15-24 depend from independent claims 1 and 14, respectively, and incorporate the limitations thereof. The Examiner's argument assumes that Roh and Atkins disclose all elements of claims 1 and 14 which are incorporated in dependent claims 2-13 and 15-24. However, as discussed above, Roh and Atkins do not disclose all the limitations of claims 1 and 14. Furthermore, Stallings does not cure the deficiencies of Roh and Atkins. Therefore, claims 2-13 and 15-24 are not obvious in view of the cited references. Accordingly, reconsideration and withdrawal of the rejection of claims 2-13 and 15-24 are respectfully requested.

II. Request for Reference

In the outstanding Final Office Action mailed January 27, 2009 in connection with the above-identified application, although the Examiner cited "Cryptography and Network Security," by W. Stallings, 2nd Edition, 1999, to reject claims 2-13 and 15-24, the Examiner did not list the reference on the PTO-892 form enclosed with the Final Office Action.

In this connection, please furnish Applicants with a revised PTO-892 listing "Cryptography and Network Security," by W. Stallings, 2nd Edition, 1999 and send a copy of the reference.

CONCLUSION

In view of the foregoing, it is believed that all claims now pending are now in condition for allowance and such action is earnestly solicited at the earliest possible date. If there are any additional fees due in connection with the filing of this response, please charge those fees to our Deposit Account No. 02-2666. If the Examiner believes that a telephone conference would be useful in moving the application forward to allowance, the Examiner is encouraged to contact the undersigned at (310) 207 3800.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 4/27, 2009

Eric S. Hyman, Reg. No 30,139

1279 Oakmead Parkway
Sunnyvale, California 94085-4040
Telephone (310) 207-3800
Facsimile (408) 720-8383

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being submitted electronically via EFS Web to the United States Patent and Trademark Office on the date shown below.

Jessica Huester 4/27/09

Jessica Huester Date